Quantum phase uncertainty in mutually unbiased measurements and Gauss sums

Michel R. P. Planat, Haret Rosu

Quantum phase uncertainty in mutually unbiased measurements and Gauss sums

Michel Planat[a] and Haret Rosu[b]

[a]Institut FEMTO-ST, Departement LPMO,
32 Avenue de l'Observatoire, 25044 Besançon Cedex, France;
[b]Div. of Advanced Materials,
IPICyT, Apdo Postal 3-74, Tangamanga, San Luis Potosí, Mexico.

ABSTRACT

Mutually unbiased bases (MUBs), which are such that the inner product between two vectors in different orthogonal bases is constant equal to the inverse $1/\sqrt{d}$, with d the dimension of the finite Hilbert space, are becoming more and more studied for applications such as quantum tomography and cryptography, and in relation to entangled states and to the Heisenberg-Weil group of quantum optics. Complete sets of MUBs of cardinality $d+1$ have been derived for prime power dimensions $d = p^m$ using the tools of abstract algebra (Wootters in 1989, Klappenecker in 2003). Presumably, for non prime dimensions the cardinality is much less.

The bases can be reinterpreted as quantum phase states, i.e. as eigenvectors of Hermitean phase operators generalizing those introduced by Pegg & Barnett in 1989. The MUB states are related to additive characters of Galois fields (in odd characteristic p) and of Galois rings (in characteristic 2). Quantum Fourier transforms of the components in vectors of the bases define a more general class of MUBs with multiplicative characters and additive ones altogether. We investigate the complementary properties of the above phase operator with respect to the number operator. We also study the phase probability distribution and variance for physical states and find them related to the Gauss sums, which are sums over all elements of the field (or of the ring) of the product of multiplicative and additive characters.

Finally we relate the concepts of mutual unbiasedness and maximal entanglement. This allows to use well studied algebraic concepts as efficient tools in our quest of minimal uncertainty in quantum information primitives.

Keywords: Quantum phase, phase fluctuations, Galois fields, mutually unbiased bases

1. INTRODUCTION

In quantum mechanics, orthogonal bases of a Hilbert space $\mathcal{H}_q$ of finite dimension q are mutually unbiased if inner products between all possible pairs of vectors of distinct bases equal $1/\sqrt{q}$. They are also said to be maximally non commutative in the sense that a measurement over one basis leaves one completely uncertain as to the outcome of a measurement performed over a basis unbiased to the first. Eigenvectors of ordinary Pauli spin matrices (i.e. in dimension $q = 2$) provide the best known example. With a complete set of $q + 1$ mutually unbiased measurements one can ascertain the density matrix of en ensemble of unknown quantum q-states, so that a natural question emerges as which mathematics may provide the construction. It will be shown that in dimension $q = p^m$ which is the power of a prime p, the complete sets of mutually unbiased bases (MUBs) result from Fourier analysis over a Galois field F_q (in odd characteristic p)[1] or of Galois ring R_{4^m} (in even characteristic 2)[2] . An exhaustive literature on MUBs can be found in[3] ,[4] . Complete sets of MUBs have an intrinsic geometrical interpretation, and were related to discrete phase spaces[3] ,[5] ,[6] , finite projective planes[7] ,[8] , convex polytopes[9] , and complex projective 2-designs[10] ,[11] . The last paper points out the relation to symmetric informationally complete positive operator measures (SIC-POVMs)[12] ,[13] ,[14] and to Latin squares[15] .

Further author information: (Send correspondence to Michel Planat)
Michel Planat: E-mail: planat@lpmo.edu, Telephone: 33 3 81 85 39 57

A Galois field is a finite set structure endowed with two group operations, the addition "+" and the multiplication "·". The field F_q can be represented as classes of polynomials obtained by computing modulo an irreducible polynomial over the ground field $F_p = \mathcal{Z}_p$, the integers modulo p.[16] A Galois field exists if and only if (iff) $q = p^m$.

A character $\kappa(g)$ over an abelian group G is a (continuous) map from G to the field of complex numbers $\mathcal{C}$, which is of modulus 1, i.e. such that $|\kappa(g)| = 1$, $g \in G$. The multiplicative characters $\psi_k(n) = \exp(\frac{2i\pi nk}{q})$, $k = 0..q-1$ are well known since they constitute the basis for the ordinary discrete Fourier transform. But the additive characters introduced below are the ones which are useful to construct the MUBs. This construction is implicit in some previous papers,[1],[2],[4] and is now being fully recognized[17] ,[18] .

An interesting consequence is as follows: the discrete Fourier transform in $\mathcal{Z}_q$ has been used as a definition of phase states $|\theta_k\rangle$, $k = 0..q-1$ in $\mathcal{H}_q$. The phase states[19] could be considered as eigenvectors of a properly defined Hermitian phase operator Θ. Phase properties and phase fluctuations attached to particular field states were extensively described. In particular the classical phase variance $\pi^2/3$ could be recovered. Similarly a phase operator Θ_{Gal} having the MUBs as eigenvectors will be constructed here, but in contrast to the case of Θ, phase fluctuations from Θ_{Gal} can in principle be reduced, a result which reflects the property of Gauss sums over F_q, and which confirms the interest of MUBs for quantum signal processing. Character sums and Gauss sums which are useful for optimal bases of m-qudits (p odd) will be also generalized to optimal bases of m-qubits ($p = 2$).

It is worthwhile to mention that quadratic Gauss sums were already met in the transient and revival dynamics of semi-classical wave packets[20] . Finally, related exponential sums: Ramanujan sums and Kloosterman sums were found to control the phase dynamics of quantum phase-locked states[21] .

2. SOME CHARACTER SUMS OVER A GALOIS FIELD

Let us consider the field of polynomials $F_p[x]$ defined over the field F_p

$$F_p[x] = \{a_0 + a_1 x + \cdots + a_n x^n\}, \quad a_i \in F_p. \tag{1}$$

For a polynomial $g \in F_p[x]$, the residue class ring $F_p[x]/(g)$, where (g) is the ideal class generated by g is a field iff g is irreducible over F_p (it cannot be factored over F_p).

For example for $q = 2^2$, one can choose the polynomial $g(x) = x^2 + x + 1 \in F_2[x]$ which is irreducible over F_2. Contrary to $\mathcal{Z}_4$ which has zero divisors and is thus only a ring, the above construction defines the field with four residue classes: $F_4 = \{0, 1, x, x+1\}$.

The key relation between Galois fields F_q and mutually unbiased bases is the theory of characters. It starts from a map from the extended field F_q to the ground field F_p which is called the trace function

$$tr(x) = x + x^p + \cdots + x^{p^{m-1}} \in F_p, \quad \forall\, x \in F_q. \tag{2}$$

In addition to its property of mapping an element of F_q into F_p, the trace function has the properties

$$\begin{gathered} tr(x+y) = tr(x) + tr(y), \quad x, y \in F_q \\ tr(ax) = a tr(x), \quad x \in F_q,\ a \in F_p, \\ tr(a) = ma, \quad a \in F_p, \\ tr(x^q) = tr(x), \quad x \in F_q. \end{gathered} \tag{3}$$

Using (2), an additive character over F_q is defined as

$$\kappa(x) = \omega_p^{tr(x)}, \quad \omega_p = \exp(\frac{2i\pi}{p}), \quad x \in F_q. \tag{4}$$

It satisfies $\kappa(x+y) = \kappa(x)\kappa(y)$, $x, y \in F_q$.

The multiplicative characters are

$$\psi_k(n) = \exp(\frac{2i\pi nk}{q}), \quad k = 0..q-1, \quad k = 0..q-1. \tag{5}$$

The construction of MUBs will be related to character sums with polynomial arguments $f(x)$ also called Weil sums[2]

$$\sum_{x \in F_q} \kappa(f(x)). \tag{6}$$

In particular (theorem 5.38 in[16]), for a polynomial $f(x) \in F_q[x]$ of degree $d \geq 1$, with $gcd(d,q) = 1$, one gets $|\sum_{x \in F_q} \kappa(f(x))| \leq (d-1)q^{1/2}$.

Finally, the phase fluctuations arising from MUBs (quantum phase states) will be found to be related to the Gauss sums of the form

$$G(\psi, \kappa) = \sum_{x \in F_q^*} \psi(x)\kappa(x). \tag{7}$$

Using the notation ψ_0 for a trivial multiplicative character $\psi = 1$, and κ_0 for a trivial additive character $\kappa = 1$ the Gaussian sums (7) satisfy $G(\psi_0, \kappa_0) = q-1$; $G(\psi_0, \kappa) = -1$; $G(\psi, \kappa_0) = 0$ and $|G(\psi, \kappa)| = q^{1/2}$ for nontrivial characters κ and ψ.

We also mention that more general Gauss sums were studied as

$$G(\psi, \kappa) = \sum_{x \in F_q} \psi(f(x))\kappa(g(x)), \tag{8}$$

with $f, g \in F_q[x]$ and found to be of the order of magnitude $\sqrt{q}$ ([16] p. 249).

3. MUTUALLY UNBIASED BASES OF QUANTUM PHASE STATES (IN ODD PRIME CHARACTERISTIC)

Let us introduce a class of quantum states as a "Galois" Fourier transform

$$|\theta^{(y)}\rangle = \frac{1}{\sqrt{q}} \sum_{n \in F_q} \psi(n)\kappa(yn)|n\rangle, \quad y \in F_q \tag{9}$$

in which the coefficient in the computational base $\{|0\rangle, |1\rangle, \cdots, |q-1\rangle\}$ represents the product of an arbitrary multiplicative character $\psi_k(n)$ by an arbitrary additive character $\kappa(yn)$.

3.1. Pegg & Barnett 89

For $\kappa = \kappa_0$ and $\psi \equiv \psi_k(n)$, one recovers the ordinary quantum Fourier transform over $\mathcal{Z}_q$. It has been shown[19] that the corresponding states

$$|\theta_k\rangle = \frac{1}{\sqrt{q}} \sum_{n \in \mathcal{Z}_q} \psi_k(n)|n\rangle, \tag{10}$$

are eigenstates of the Hermitian phase operator

$$\Theta = \sum_{k \in \mathcal{Z}_q} \theta_k |\theta_k\rangle\langle\theta_k|, \tag{11}$$

with eigenvalues $\theta_k = \theta_o + \frac{2\pi k}{q}$, θ_0 an arbitrary initial phase.

3.2. Wootters & Fields 89

We employ the Euclidean division theorem (theorem 11.19 in[22]) for the field F_q, which says that given any two polynomials y and n in F_q, there exists a uniquely determined pair $(a, b) \in F_q \times F_q$, such that $y = an + b$, $\deg(b) < deg(a)$. Using the decomposition of the exponent in (9), we obtain

$$|\theta_b^a\rangle = \frac{1}{\sqrt{q}} \sum_{n \in F_q} \psi_k(n)\kappa(an^2 + bn)|n\rangle, \quad a, b \in F_q. \tag{12}$$

This defines a set of q bases (with index a) of q vectors (with index b). Using Weil sums (6) it is easily shown that, for q odd, so that $\gcd(2, \mathrm{q}) > 1$, the bases are orthogonal and mutually unbiased to each other and to the computational base. More precisely

$$|\langle\theta_b^a|\theta_d^c\rangle| = |\frac{1}{q} \sum_{n \in F_q} \omega_p^{tr((c-a)n^2+(d-b)n}| = \begin{cases} \delta_{bd} & \text{if } c = a \text{ (orthogonality)} \\ \frac{1}{\sqrt{q}} & \text{if } c \neq a \text{ (unbiasedness).} \end{cases} \tag{13}$$

The MUB states are also eigenstates of a “Galois” quantum phase operator

$$\Theta_{\mathrm{Gal}} = \sum_{b \in F_q} \theta_b |\theta_b^a\rangle\langle\theta_b^a|, \quad a, b \in F_q. \tag{14}$$

with eigenvalues $\theta_b = \frac{2\pi b}{q}$.

4. QUANTUM PHASE FLUCTUATIONS FROM MUBS (IN ODD PRIME CHARACTERISTIC)

4.1. The Galois operator

Using (12) in (14) and the properties of the field theoretical trace (3), the Galois operator reads

$$\Theta_{\mathrm{Gal}} = \frac{2\pi}{q^2} \sum_{m,n \in F_q} \psi_k(n-m)\omega_p^{tr[a(n^2-m^2)]} S(n,m)|n\rangle\langle m|, \quad \text{with } \mathrm{S(n,m)} = \sum_{\mathrm{b \in F_q}} \mathrm{b}\omega_{\mathrm{p}}^{\mathrm{tr[b(n-m)]}}. \tag{15}$$

In the diagonal matrix elements, we have the partial sums

$$S(n,n) = \frac{q(q-1)}{2}, \tag{16}$$

so that $\langle n|\Theta_{\mathrm{Gal}}|n\rangle = \frac{\pi(q-1)}{q}$. In the non-diagonal matrix elements, the partial sums can be calculated from

$$\sum_{b \in F_q} bx^b = x(1 + 2x + 3x^2 + \cdots + qx^{q-1}) = x[\frac{1-x^q}{(1-x)^2} - \frac{qx^q}{1-x}] = \frac{xq}{x-1}, \tag{17}$$

where we introduced $x = \omega_p^{tr(n-m)}$ and we made use of the relation $x^q = 1$. Finally

$$S(m,n) = \frac{q}{1 - \omega_p^{tr(m-n)}}. \tag{18}$$

4.2. The Galois phase-number commutator

Using (15) and the number operator

$$N = \sum_{l \in F_q} l|l\rangle\langle l|, \tag{19}$$

the matrix elements of the phase-number commutator $[\Theta_{\mathrm{Gal}}, N]$ are calculated as

$$u_{\mathrm{Gal}}(n,m) = \frac{2\pi}{q^2}(n-m)\psi_k(n-m)\omega_p^{tr[a(n^2-m^2)]} S(n,m). \tag{20}$$

The diagonal elements vanish, the corresponding matrix is antihermitian since $u_{\mathrm{Gal}}(n,m) = -u^\dagger_{\mathrm{Gal}}(m,n)$, and the states are pseudo-classical since $\lim_{q\to\infty} u_{\mathrm{Gal}}(n,m) = 0$.

4.3. Galois phase expectation value and variance

For the evaluation of phase properties of MUB states we consider a pure phase state of the form

$$|f\rangle = \sum_{n\in F_q} u_n|n\rangle, \quad \text{with } \mathrm{u_n} = \frac{1}{\sqrt{\mathrm{q}}}\exp(\mathrm{in}\beta), \tag{21}$$

where β is a real parameter, and we compute respectively the phase probability distribution, the phase expectation value and the phase variance as

$$\begin{gathered} |<\theta_b|f>|^2, \\ <\Theta_{\mathrm{Gal}}>=\textstyle\sum_{b\in F_q}\theta_b|<\theta_b|f>|^2, \\ <\Delta\Theta^2_{\mathrm{Gal}}>=\textstyle\sum_{b\in F_q}(\theta_b-<\Theta_{\mathrm{Gal}}>)^2|<\theta_b|f>|^2, \end{gathered} \tag{22}$$

where the upper index a for the base is implicit and we omitted it for simplicity.

4.4. Phase expectation value

The two factors in the expression for the probability distribution

$$\frac{1}{q^2}[\sum_{n\in F_q}\psi_k(-n)\exp(in\beta)\omega_p^{-tr(an^2+bn)}][\sum_{m\in F_q}\psi_k(m)\exp(-im\beta)\omega_p^{tr(am^2+bm)}], \tag{23}$$

have absolute values bounded by the absolute value of generalized Gauss sums (8), so that the overall bound is

$$|<\theta_b|f>|^2 \le \frac{1}{q}. \tag{24}$$

It follows that the absolute value of the phase expectation value is bounded as it is expected for an arbitrary phase factor.

$$|<\Theta_{\mathrm{Gal}}>| \le \frac{2\pi}{q^2}\sum_{b\in F_q} b \le \pi. \tag{25}$$

More precisely the phase expectation value can be expressed as

$$<\Theta_{\mathrm{Gal}}>=\frac{2\pi}{q^3}\sum_{m,n\in F_q}\psi_k(m-n)\exp[i(n-m)\beta]\omega_p^{tr[a(m^2-n^2]}S(m,n). \tag{26}$$

where the sums $S(m,n)$ were defined in (16) and (18). All the q diagonal terms $m=n$ in $<\Theta_{\mathrm{Gal}}>$ contribute an order of magnitude $\frac{2\pi}{q^3}qS(n,n)\simeq\pi$. The contribution of off-diagonal terms and possible cancellation of phase oscillations could be considered from numerical plots, since the sums in (26) are not easy to evaluate analytically.

4.5. Phase variance

The phase variance can be written as

$$<\Delta\Theta^2_{\mathrm{Gal}}>=\sum_{b\in F_q}(\theta_b^2-2\theta_b<\Theta_{\mathrm{Gal}}>)|<\theta_b|f>|^2, \tag{27}$$

The coefficient $<\Theta_{\mathrm{Gal}}>^2\sum_{b\in F_q}|<\theta_b|f>|^2$ doesn't contribute since it is proportional to the Weil sum $\sum_{b\in F_q}\omega_p^{tr(b(n-m)}=0$. As a result a cancellation of phase fluctuations may occur in (27) from to the two extra terms of opposite sign.

But the calculation are again not easy to perform analytically. For the first term one gets

$$\frac{4\pi^2}{q^4}\sum_{m,n\in F_q}\psi_k(m-n)\exp[i(n-m)\beta]\omega_p^{tr[a(m^2-n^2)]}T(m,n), \quad \text{with } \mathrm{T(n,m)}=\sum_{\mathrm{b\in F_q}}\mathrm{b}^2\omega_{\mathrm{p}}^{\mathrm{tr[b(n-m)]}}. \tag{28}$$

In the diagonal elements we have the partial sums

$$T(n,n) = \sum_{b \in F_q} b^2 = \frac{q^3}{3} - \frac{q^2}{2} + \frac{q}{6}. \tag{29}$$

In the non-diagonal terms the partial sums can be calculated from

$$\sum_{b \in F_q} b^2 x^b = x(1 + 2^2 x + 3^2 x^2 + \cdots + (q-1)^2 x^{q-1}) = x\frac{d}{dx}\{x[\frac{1-x^q}{(1-x)^2} - \frac{qx^q}{1-x}]\} = \frac{-2qx}{(1-x)^2}, \tag{30}$$

where we introduced $x = \omega_p^{tr(n-m)}$ and we made use of the relations $x^q = 1$ and $q^2 = 0$.

The second term in (27) is

$$\sum_{b \in F_q} -2\theta_b < \Theta_{\text{Gal}} > | < \theta_b | f > |^2 = -2 < \Theta_{\text{Gal}} >^2 . \tag{31}$$

Partial cancellation occurs in diagonal terms of (27) since the contribution is

$$\frac{4\pi^2}{q^4} q T(n,n) - \frac{8\pi^2}{q^4} S(n,n)^2 \simeq \frac{4\pi^2}{3} - 2\pi^2 = -\frac{2\pi^2}{3}, \tag{32}$$

which is still twice (in absolute value) the amount of phase fluctuations in the classical regime. It is expected that cancellations also occur in the non-diagonal terms to beat the classical limit, as for the case of squeezed states.

5. GALOIS RINGS AND THEIR CHARACTER SUMS

5.1. Construction of the Galois rings of characteristic 4

The Weil sums (6) which have been proved useful in the construction of MUB's in odd characteristic p (and odd dimension $q = p^m$), are not useful in characteristic $p = 2$, since in this case the degree 2 of polynomial $f(x)$ is such that gcd(2, q)=0.

An elegant method for constructing complete sets of MUBs of m-qubits was found[2] . It makes use of objects of the context of quaternary codes[23] , the so-called Galois rings R_{4^m}. In contrast to the Galois fields where the ground alphabet has p elements (p a prime number) in the field $F_p = \mathcal{Z}_p$, the ring R_{4^m} takes its ground alphabet in $\mathcal{Z}_4$. To construct it one uses the ideal class (h), where h is a (monic) basic irreducible polynomial of degree m. It is such that its restriction to $\bar{h}(x) = h(x)\text{mod } 2$ is irreducible over $\mathcal{Z}_2$. The Galois ring R_{4^m} is defined as the residue class ring $\mathcal{Z}_4[x]/(h)$. It has cardinality 4^m.

We also needs the concept of a primitive polynomial. A (monic) primitive polynomial, of degree m, in the field $F_q[x]$ is irreducible over F_q and has a root $\alpha \in F_{q^m}$ that generates the multiplicative group of F_{q^m}. A polynomial $f \in F_q[x]$ of degree m is primitive iff $f(0) \neq 0$ and divides $x^r - 1$, with $r = q^m - 1$.

Similarly for Galois rings R_{4^m}, if $\bar{h}[x]$ is a primitive polynomial of degree m in $\mathcal{Z}_2[x]$, then there is a unique basic primitive polynomial $h(x)$ of degree m in $\mathcal{Z}_4[x]$ (it divides $x^r - 1$, with $r = 2^m - 1$). It can be found as follows.[24] Let $\bar{h}(x) = e(x) - d(x)$, where $e(x)$ contains only even powers and $d(x)$ only odd powers; then $h(x^2) = \pm(e^2(x) - d^2(x))$. For $m = 2$, 3 and 4 one takes $\bar{h}(x) = x^2+x+1$, $\bar{h}(x) = x^3+x+1$ and $\bar{h}(x) = x^4+x+1$ and one gets $h(x) = x^2 + x + 1$, $x^3 + 2x^2 + x - 1$ and $x^4 + 2x^2 - x + 1$, respectively.

Any non zero element of F_{p^m} can be expressed in terms of a single primitive element. This is no longer true in R_{4^m}, which contains zero divisors. But in the latter case there exists a nonzero element ξ of order $2^m - 1$ which is a root of the basic primitive polynomial $h(x)$. Any element $y \in R_{4^m}$ can be uniquely determined in the form $y = a + 2b$, where a and b belong to the so-called Teichmüller set $\mathcal{T}_m = (0, 1, \xi, \cdots, \xi^{2^m-2})$. Moreover, one finds that $a = y^{2^m}$. We can also define the trace to the base ring $\mathcal{Z}_4$ by the map

$$\tilde{tr}(y) = \sum_{k=0}^{m-1} \sigma^k(y), \tag{33}$$

where the summation runs over R_{4^m} and the Frobenius automorphism σ reads

$$\sigma(a+2b) = a^2 + 2b^2. \tag{34}$$

Let us apply this formula to the case $m = 2$ (which will correspond to 2-qubits). In $R_{4^2} = \mathcal{Z}_4[x]/(x^2+x+1)$ the Teichmüller set reads $\mathcal{T}_2 = (0, 1, x, 3+3x)$; the 16 elements $a+2b$ with a and b in $\mathcal{T}_2$ are shown in the following matrix

$$\begin{bmatrix} 0 & 2 & 2x & 2+2x \\ 1 & 3 & 1+2x & 3+2x \\ x & 2+x & 3x & 2+3x \\ 3+3x & 1+3x & 3+x & 1+x \end{bmatrix}. \tag{35}$$

The case $m = 3$ corresponding to 3-qubits can be examined in a similar fashion, with the ring $R_{4^3} = \mathcal{Z}_4[x]/(x^3 + 2x^2 + x - 1)$ and the Teichmüller set featuring the following eight elements: $\mathcal{T}_3 = \{0, 1, x, x^2, 1+3x+2x^2, 2+3x+3x^2, 3+3x+x^2, 1+2x+x^2\}$.

In the Galois ring of characteristic 4 the additive characters are

$$\tilde{\kappa}(x) = \omega_4^{\tilde{\mathrm{tr}}(x)} = i^{\tilde{\mathrm{tr}}(x)}. \tag{36}$$

5.2. Exponential sums over R_{4^m}

The Weil sums (6) are replaced by the exponential sums[2]

$$\Gamma(y) = \sum_{u \in \mathcal{T}_m} \tilde{\kappa}(yu), \quad y \in R_{4^m} \tag{37}$$

which satisfy

$$|\Gamma(y)| = \begin{cases} 0 \ \text{ if } y \in 2\mathcal{T}_m,\ y \neq 0 \\ 2^m \ \text{ if } y = 0 \\ \sqrt{2^m} \ \text{ otherwise.} \end{cases} \tag{38}$$

Gauss sums for Galois rings were constructed[25]

$$G_y(\tilde{\psi}, \tilde{\kappa}) = \sum_{x \in R_{4^m}} \tilde{\psi}(x)\tilde{\kappa}(yx), \quad y \in R_{4^m}, \tag{39}$$

where the multiplicative character $\bar{\psi}(x)$ can be made explicit[25] .

Using the notation $\bar{\psi}_0$ for a trivial multiplicative character and $\tilde{\kappa_0}$ for a trivial additive character, the Gaussian sums (39) satisfy $G(\tilde{\psi_0}, \tilde{\kappa_0}) = 4^m$; $G(\tilde{\psi}, \tilde{\kappa_0}) = 0$ and $|G(\tilde{\psi}, \tilde{\kappa})| \leq 2^m$.

6. MUTUALLY UNBIASED BASES OF QUANTUM PHASE STATES (M-QUBITS)

The quantum phase states for m-qubits can be found as the "Galois ring" Fourier transform

$$|\theta^{(y)}\rangle = \frac{1}{\sqrt{2^m}} \sum_{n \in \mathcal{T}_m} \tilde{\psi}(n)\tilde{\kappa}(yn)|n\rangle, \quad y \in R_{4^m}. \tag{40}$$

6.1. A. Klappenecker & M. Rötteler 03

It was shown in the previous section that each element y of the ring R_{4^m} decomposes as $y = a + 2b$, a and b in the Teichmüller set $\mathcal{T}_m$. Using this result in the character function $\tilde{\kappa}$ one obtains

$$|\theta_b^a\rangle = \frac{1}{\sqrt{2^m}} \sum_{n \in \mathcal{T}_m} \tilde{\psi}_k(n)\tilde{\kappa}[(a+2b)n]|n\rangle, \quad a, b \in \mathcal{T}_m. \tag{41}$$

This defines a set of 2^m bases (with index a) of 2^m vectors (with index b). Using the exponential sums (37), it is easy to show that the bases are orthogonal and mutually unbiased to each other and to the computational base. The case $\bar{\psi} \equiv \bar{\psi}_0$ was obtained before[2] .

6.2. MUB's for m-qubits, $m = 1$, 2 and 3

For the special case of qubits, one uses $\tilde{\mathrm{tr}}(x) = x$ in (41) so that the three pairs of MUB's are given as

$$[|0\rangle, |1\rangle]; \quad \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle, |0\rangle - |1\rangle]; \quad \frac{1}{\sqrt{2}}[|0\rangle + i|1\rangle, |0\rangle - i|1\rangle]. \tag{42}$$

For 2-qubits one gets a complete set of 5 bases

$$\begin{array}{c}
(|0\rangle, |1\rangle, |2\rangle, |3\rangle); \\
\frac{1}{2}[|0\rangle + |1\rangle + |2\rangle + |3\rangle, |0\rangle + |1\rangle - |2\rangle - |3\rangle, |0\rangle - |1\rangle - |2\rangle + |3\rangle, |0\rangle - |1\rangle + |2\rangle - |3\rangle] \\
\frac{1}{2}[|0\rangle - |1\rangle - i|2\rangle - i|3\rangle, |0\rangle - |1\rangle + i|2\rangle + i|3\rangle, |0\rangle + |1\rangle + i|2\rangle - i|3\rangle, |0\rangle + |1\rangle - i|2\rangle + i|3\rangle] \\
\frac{1}{2}[|0\rangle - i|1\rangle - i|2\rangle - |3\rangle, |0\rangle - i|1\rangle + i|2\rangle + |3\rangle, |0\rangle + i|1\rangle + i|2\rangle - |3\rangle, |0\rangle + i|1\rangle - i|2\rangle + |3\rangle] \\
\frac{1}{2}[|0\rangle - i|1\rangle - |2\rangle - i|3\rangle, |0\rangle - i|1\rangle + |2\rangle + i|3\rangle, |0\rangle + i|1\rangle + |2\rangle - i|3\rangle, |0\rangle + i|1\rangle - |2\rangle + i|3\rangle],
\end{array} \tag{43}$$

and for 3 qubits a complete set of 9 bases

$$\begin{array}{c}
(|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle); \\
\frac{1}{4}[|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle, |0\rangle + |1\rangle - |2\rangle + |3\rangle - |4\rangle - |5\rangle - |6\rangle + |7\rangle, \\
|0\rangle - |1\rangle + |2\rangle - |3\rangle - |4\rangle - |5\rangle + |6\rangle - |7\rangle, |0\rangle + |1\rangle - |2\rangle - |3\rangle - |4\rangle + |5\rangle + |6\rangle - |7\rangle, \\
|0\rangle - |1\rangle - |2\rangle - |3\rangle + |4\rangle + |5\rangle - |6\rangle + |7\rangle, |0\rangle - |1\rangle - |2\rangle + |3\rangle + |4\rangle - |5\rangle + |6\rangle - |7\rangle, \\
|0\rangle - |1\rangle + |2\rangle + |3\rangle - |4\rangle + |5\rangle - |6\rangle - |7\rangle, |0\rangle + |1\rangle + |2\rangle - |3\rangle + |4\rangle - |5\rangle - |6\rangle - |7\rangle], \\
\cdots
\end{array} \tag{44}$$

where only the first two bases have been printed for simplicity.

6.3. Quantum phase fluctuations for m-qubits

Quantum phase states of m-qubits (41) derive from a "Galois ring" quantum phase operator as in (14), and calculations similar to those performed in Sect. (4) can be done, since the $\tilde{\mathrm{tr}}$ operator (33) follows rules similar to the tr operator (2). In analogy to the case of qdits in dimension p^m, p an odd prime, phase properties for sets of m-qubits heavily rely on the Gauss sums (39). As before the calculations are tedious but can in principle be achieved in specific cases.

7. MUTUAL UNBIASEDNESS AND MAXIMAL ENTANGLEMENT

It has been shown in this paper that there is a founding link between irreducible polynomials over a ground field F_p and complete sets of mutually unbiased bases arising from Fourier transform over a lifted field F_q, $q = p^m$, p a prime number. On the other hand the physical concept of entanglement over the Hilbert space $\mathcal{H}_q$ evokes irreducibility. Roughly speaking entangled states in $\mathcal{H}_q$ cannot be factored into tensorial products of states in Hilbert spaces of lower dimension. We show now that there is an intrinsic relation between MUBs and maximal entanglement.

We are familiar we the Bell states

$$\begin{aligned}
(|\mathcal{B}_{0,0}\rangle, |\mathcal{B}_{0,1}\rangle) &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle, |00\rangle - |11\rangle), \\
(|\mathcal{B}_{1,0}\rangle, |\mathcal{B}_{1,1}\rangle) &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle, |01\rangle - |10\rangle),
\end{aligned}$$

where a compact notation $|00\rangle = |0\rangle \odot |0\rangle$, $|01\rangle = |0\rangle \odot |1\rangle$,..., is employed for the tensorial products.

These states are both orthonormal and maximally entangled, such that $trace_2|\mathcal{B}_{h,k}\rangle\langle\mathcal{B}_{h,k}| = \frac{1}{2}I_2$, where $trace_2$ means the partial trace over the second qubit[26] .

One can define more generalized Bell states using the multiplicative Fourier transform (10) applied to the tensorial products of two qudits[28] ,[17]

$$|\mathcal{B}_{h,k}\rangle = \frac{1}{\sqrt{q}}\sum_{n=0}^{q-1}\omega_q^{kn}|n, n+h\rangle, \tag{45}$$

These states are both orthonormal, $\langle\mathcal{B}_{h,k}|\mathcal{B}_{h',k'}\rangle = \delta_{hh'}\delta_{kk'}$, and maximally entangled, $trace_2|\mathcal{B}_{h,k}\rangle\langle\mathcal{B}_{h,k}| = \frac{1}{q}I_q$.

But we can also define a more general class of maximally entangled states using the Fourier transform over F_q (12) as follows

$$|\mathcal{B}_{h,b}^a\rangle = \frac{1}{\sqrt{q}}\sum_{n=0}^{q-1}\omega_p^{tr[(an+b)n]}|n, n+h\rangle, \tag{46}$$

A list of the generalized Bell states of qutrits for the base $a = 0$ can be found in[27] , the work that relies on a coherent state formulation of entanglement. In general, for q a power of a prime, starting from (46) one obtains q^2 bases of q maximally entangled states. Each set of the q bases (with h fixed) has the property of mutual unbiasedness.

Similarly for sets of maximally entangled m-qubits one uses the Fourier transform over Galois rings (41) so that

$$|\mathcal{B}_{h,b}^a\rangle = \frac{1}{\sqrt{2^m}}\sum_{n=0}^{2^m-1} i^{tr[(a+2b)n]}|n, n+h\rangle. \tag{47}$$

For qubits ($m = 1$) one gets the following bases of maximally entangled states (in matrix form, safe for the proportionality factor)

$$\left[\begin{array}{cc} (|00\rangle+|11\rangle, |00\rangle-|11\rangle); & (|01\rangle+|10\rangle, |01\rangle-|10\rangle) \\ (|00\rangle+i|11\rangle, |00\rangle-i|11\rangle); & (|01\rangle+i|10\rangle, |01\rangle)-i|10\rangle) \end{array}\right]. \tag{48}$$

Two bases in one column are mutually unbiased, while vectors in two bases on the same line are orthogonal to each other.

For 2-particle sets of quartits, using Eqs.(43) and (47), one gets 4 sets ($|\mathcal{B}_{h,b}^a\rangle$, $h = 0, ..., 3$) of 4 MUBs ($a = 0, ..., 3$)

$$\begin{gathered}
\{(|00\rangle+|11\rangle+|22\rangle+|33\rangle, |00\rangle+|11\rangle-|22\rangle-|33\rangle, \\
|00\rangle-|11\rangle-|22\rangle+|33\rangle, |00\rangle-|11\rangle+|22\rangle-|33\rangle); \\
(|00\rangle-|11\rangle-i|22\rangle-i|33\rangle, |00\rangle-|11\rangle+i|22\rangle+i|33\rangle, \\
|00\rangle+|11\rangle+i|22\rangle-i|33\rangle, |00\rangle+|11\rangle-i|22\rangle+i|33\rangle); \\
\cdots\}
\end{gathered}$$

$$\begin{gathered}
\{(|01\rangle+|12\rangle+|23\rangle+|30\rangle, |01\rangle+|12\rangle-|23\rangle-|30\rangle, \\
|01\rangle-|12\rangle-|23\rangle+|30\rangle, |01\rangle-|12\rangle+|23\rangle-|30\rangle); \\
(|01\rangle-|12\rangle-i|23\rangle-i|30\rangle, |01\rangle-|12\rangle+i|23\rangle+i|30\rangle, \\
|01\rangle+|12\rangle+i|23\rangle-i|30\rangle, |01\rangle+|12\rangle-i|23\rangle+i|30\rangle); \\
\cdots\}
\end{gathered}$$

$$\begin{gathered}
\{(|02\rangle+|13\rangle+|20\rangle+|31\rangle, |02\rangle+|13\rangle-|20\rangle-|31\rangle, \\
|02\rangle-|13\rangle-|20\rangle+|31\rangle, |02\rangle-|13\rangle+|20\rangle-|31\rangle); \cdots \\
\cdots\}
\end{gathered}$$

$$\{(|03\rangle + |10\rangle + |21\rangle + |32\rangle, |03\rangle + |10\rangle - |21\rangle - |32\rangle,$$
$$|03\rangle - |10\rangle - |21\rangle + |32\rangle, |03\rangle - |10\rangle + |21\rangle - |32\rangle); \cdots$$
$$\cdots\}, \tag{49}$$

where, for the sake of brevity, we omitted the normalization factor (1/2). Within each set, the four bases are mutually unbiased, as in (43), while the vectors of the bases from different sets are orthogonal.

As a conclusion one found that the two related concepts of mutual unbiasedness and maximal entanglement derive from the study of lifts of the base field $\mathcal{Z}_p$ to Galois fields of prime characteristic $p > 2$ (in odd dimension), or of lifts of the base ring $\mathcal{Z}_4$ to Galois rings of characteristic 4 (in even dimension). One wonders if lifts to more general algebraic structures would play a role in the study of non maximal entanglement. We have first in mind the nearfields also useful for deriving efficient classical codes and which have a strong underlying geometry.

REFERENCES

1. W.K. Wootters and B.D. Fields, *Optimal state-determination by mutually unbiased measurements* , Ann. of Phys. **191**, 363 (1989).
2. A. Klappenecker and M. Rötteler, *Constructions of mutually unbiased bases*, Proc. Applications of Finite Fields, Fq7 (2003); e-print quant-ph/0309120 (2003).
3. K.S. Gibbons, M.J. Hoffman and W.K. Wootters, *Discrete phase space based on finite fields*, Phys. Rev. A **70**, 062101 (2004); e-print quant-ph/0401155 (2004).
4. M. Planat, H. Rosu, S. Perrine and M. Saniga, *Finite algebraic geometry underlying mutually unbiased quantum measurements*, e-print quant-ph/0409081, (2004).
5. J. Paz, A.J. Roncaglia and M. Saraceno, *Qubits in phase space: Wigner function approach to quantum error correction and the mean king problem*, eprint quant-ph/0410117.
6. A.O. Pittinger and M.H. Rubin, *Wigner Functions and Separability for Finite Systems*, eprint quant-ph/0501104.
7. M. Saniga, M. Planat and H. Rosu, J. Opt. B: Quantum Semiclass. Opt **6**,L19 (2004), *Mutually Unbiased Bases and Finite Projective Planes*, math-ph/0403057 (29 Mar 2004).
8. M. Saniga and M. Planat, *Sets of Mutually Unbiased Bases as Arcs in Finite Projective Planes?*, eprint quant-ph/0409184.
9. I. Bengtsson and A. Ericsson, *Mutually Unbiased Bases and The Complementarity Polytope*, eprint quant-ph/0410120.
10. H. Barnum, *Information-disturbance tradeoff in quantum measurement on the uniform ensemble and on the mutually unbiased bases*, eprint quant-ph/0205155.
11. A. Klappenecker and M. Roetteler, *Mutually Unbiased Bases are Complex Projective 2-Designs*, eprint quant-ph/0502031.
12. W.K. Wootters, *Quantum Measurements and Finite Geometry*, Found. of Physics (to appear); quant-ph/0406032 (4 Jun 2004).
13. M. Grassl, *On SIC-POVMs and MUBs in Dimension 6*, eprint quant-ph/0406175.
14. D. M. Appleby, *SIC-POVMs and the Extended Clifford Group*, eprint quant-ph/0412001.
15. P. Wocjan and T. Beth, *New Construction of Mutually Unbiased Bases in Square Dimensions*, quant-ph/0407081 (12 Jul 2004).
16. R. Lidl and H. Niederreiter, *Finite fields* (Addison-Wesley, Reading, Mass, 1983).
17. T. Durt, *A new expression for mutually unbiased bases in prime power dimensions*, eprint quant-ph/0409090.
18. A.B. Klimov, L.L. Sanchez-Soto and H. de Guise, *Multicomplementary operators via finite Fourier transform*, eprint quant-ph/0410155.
19. D.T. Pegg and S.M. Barnett, *Phase properties of the quantized single-mode electromagnetic field*, Phys. Rev. A **15**, 1665 (1989).
20. M. Berry, I. Marzoli and W. Schleich, *Quantum carpets, carpets of light*, Physics World, June 2001, 39 (2001).

21. M. Planat and H. Rosu, *The hyperbolic, the arithmetic and the quantum phase*, J. of Opt. B, Quant. and Semiclass. Opt. **6**, S583 (2004), e-print math-ph/0309022.
22. R. Lidl and G. Pilz, *Applied Abstract Algebra*, Second Edition (Springer Verlag, New York, 1998).
23. Z.X. Wan, *Quaternary Codes* (World Scientific, Singapore, 1997).
24. A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Sole, *The $\mathcal{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory **40**, 301 (1994).
25. Yunchang Oh and Heung-Joon Oh, *Gauss sums over Galois rings of characteristic* 4, Kangweon-Kyungki Math. Jour. **9**, 1-7 (2001).
26. M.A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000), p. 582.
27. K. Fujii, *A Relation between Coherent States and Generalized Bell States*,e-print quant-ph/0105077 (2001).
28. N.J. Cerf, M. Bourennane, A. Karlsson and N. Gisin,*Security of quantum-key distribution using d-level systems*, Phys. Rev. Lett. **88**, 127902 (2002).